УДК 621. 391:519.2:519.7

МЕТОДИ ПРОТИДІЇ АТАКАМ НА РЕАЛІЗАЦІЇ, ЯКІ БАЗУЮТЬСЯ НА АНАЛІЗІ ЕНЕРГОСПОЖИВАННЯ, СХЕМИ НАПРАВЛЕНОГО ШИФРУВАННЯ У КІЛЬЦЯХ ЗРІЗАНИХ ПОЛІНОМІВ

Д.В. ІВАНЕНКО

Аналіз існуючих методів протидії атакам спеціального виду. Досліджуються недоліки та переваги методів протидії атакам: CPA, SPA, DPA, які реалізуються на криптосистеми у кільцях зрізаних поліномів.

Ключові слова: методи протидії, атаки спеціального виду, CPA, DPA, SPA.

ВСТУП

Відсутність нових відкритих публікацій про переваги та недоліки математичної моделі сучасних асиметричних криптосистем, при існуванні відомих успішних реалізації на схеми направленого шифрування, наводить на думку науковий світ, що зловмисники звернули увагу безпосередньо на програмну та апаратну реалізацію. Тобто завдання зловмисника зводиться до дослідження реалізованої криптосистеми з метою пошуку залежностей, переваг та недоліків; гонка за швидкістю, великою продуктивністю за рахунок оптимізації, використання сучасних технологій – веде до складностей при апаратній реалізації, людського фактору – помилок у реалізації, все це веде до імовірності реалізації атак [3] на реалізацію.

Такі атаки отримали назву атаки спеціального виду, існування таких атак формулює завдання аналізу існуючих та можливих методів протидії атакам спеціального виду. В цій роботі будуть проаналізовані методи боротьби з атаками, які базуються на аналізі енергоспоживання, та зроблено спробу запропонувати універсальний метод.

1. ІСНУЮЧІ МЕТОДИ ПРОТИДІЇ АТАКАМ НА РЕАЛІЗАЦІЇ

З появою атак спеціального виду виникла задача створити методи та засоби протидії цим атакам. Наведемо класифікацію та дамо визначення таким методам протидії:

1) Використання фіксованих схем операції для кожної моделі операції:

а) Метод Монтгомері [6–9]. Цей метод дозволяє прискорити операцію множення та піднесення до квадрата;

б) Доповнення до операцій [10–13]. До основної групи операції додаються змішані додавання, фіксовані додавання, єдині додавання, подвоєння;

в) Атомарність [14]. Це властивість операцій, під якою розуміють, що операція виконується як єдине ціле або не виконується взагалі. Тобто, внаслідок порушення процедури виконання операції, процедура виконання відкочується до початку операції і всі операнди операції генеруються спочатку.

2) Рандомізація даних [5];

3) Засліплення даних [15–17]. Засліплення служить для зміни вхідних даних у деякий непередбачуваний стан. Залежно від характеристик функції засліплення, вона може виключити деякі або всі витоки корисної інформації.

Складність вибору методу протидії ускладнюється ще тим, що атака спеціального виду є атакою окремого випадку. Тобто успішна реалізація на одному пристрої може бути неефективною для іншого пристрою.

Також з впровадженням методу протидії потрібно враховувати особливість системи, для того щоб реалізація методу протидії не впливала на ефективність та на властивості, за якими було обрано криптоперетворення.

2. КРИПТОСИСТЕМА З ВІДКРИТИМ КЛЮЧЕМ NTRU

Для аналізу методів протидії атакам спеціального виду обрали схему направленого шифрування у кільцях зрізаних поліномів, NTRU. Тому що саме в NTRU бачать світле майбутнє у постквантовій криптографії.

Алгоритм включає в себе три відкритих параметри (N, q, p), де N, q, p – цілі, та q, p – взаємно прості при тому, що p значно менше від q. Процедура генерації ключа починається з вибору випадкового $F \in R$ та вирахування $f:=1+pF$. У випадку, якщо f не має зворотного елемента за *mod q*, то потрібно обрати інший F та повторити процедуру. Далі необхідно вибрати другий поліном $g \in R$, який буде зворотний за *mod q*. Таким чином, f – це секретний ключ, а h – відкритий ключ, який потрібно обчислити з такого виразу: $h:=pf^{-1} *g \bmod q$. Повідомлення позначається через m. При шифруванні відправник випадково вибирає поліном $r \in R$, потім обчислює значення шифр-тексту $e:=r*h+m \bmod q$. Для розшифрування e отримувач обчислює $a:=f*e \bmod A\ q$, де *modA q* означає, що коефіцієнти зсуваються на інтервал $[A, A+q-1]$ після приведення за *mod q*. Потім отримувач відновлює текст за формулою – $m:=a \bmod p$.

Домінуючою операцією в шифруванні та розшифруванні NTRU вважається обчислення $r*h \bmod q$ та $f*e \bmod q$. Коефіцієнти поліномів h та

e розподілені майже випадково, один вибирає *r* та *F* так, що результат операції згортання *r*h* та *F*e* може бути мати більш низьку обчислювальну складність. В алгоритмі використовуються бінарні або тернарні коефіцієнти, r_i, $F_i \in \{0,1\}$ або {-1,0,1}, і фіксується число ненульових коефіцієнтів у *r* та *F*[18,19]. Потім обчислення операції згортання може бути обчислено за *dN*-операцією, де N – загальне число коефіцієнтів поліномів та d – число ненульових коефіцієнтів.

Алгоритм 1 є оптимізованим алгоритмом обчислення $t=a*c \bmod q$, де зниження за модулем $\bmod N$ пересуває в індексі обчислення по масиву t за рахунок додаткової пам'яті (t_N, ..., t_{2N-1}). У цьому алгоритмі, $a \in R$ є бінарним поліномом з d ненульовими коефіцієнтами та $c \in R$ – загальним поліномом. Бінарний поліном a є масивом b, у якому позначено ненульові положення d. Наприклад, $a(X)=1+x3+x6=[1,0,0,1,0,0,1,0]$ для $N=8$ матиме такий вигляд $b=[0,3,6]$.

Наприклад: розглянемо ситуацію, де зловмисник намагається відновити секретний ключ (a(x)), при тому що він контролює вхідні дані (поліном c(x)) та знає результат операції згортки (t(x)). Припущення відносно знання секретного ключа зловмисник робить за допомогою аналізу спектра енергоспоживання під час виконання операції згортки на пристрої.

Алгоритм 1 – Обчислення операції згортання [4]

Вхідне: масив b, який є не нульовим значенням бінарного поліному $a(X)$, що є секретним ключем); поліном $c(X)$.

Вихідне: $t(x)$ тимчасовий буфер, у якому зберігається результат.

1. for $0 \le j < 2N$ do
2. $t_j \leftarrow 0$ //з t_N до t_{2N-1} : тимчасовий буфер
3. end for
4. for $0 \le j < d$ do
5. for $0 \le k < N$ do
6. $t_{k+b[j]} \leftarrow t_{k+b[j]} + c_k$
7. end for
8. end for
9. for $0 \le j < N$ do
10. $t_j \leftarrow (t_j + t_{j+N}) \bmod q$
11. end for

3.ЗАПРОПОНОВАНІ МЕТОДИ ПРОТИДІЇ АТАКАМ СПЕЦІАЛЬНОГО ВИДУ НА ЕНЕРГОСПОЖИВАННЯ

Аналіз алгоритму NTRU показує, що головною математичною операцією під час зашифрування та розшифрування у алгоритмі NTRU є добуток двох поліномів $a(X)$ і $b(X)$, та операція згортання $t(X)=c(X)+a(X)$, де $a(X)$ поданий у вигляді множини b. Тому було б ефективно запропонувати методи протидії, пов'язані саме з цими операціями:

1. Рандомізація тимчасових даних, які зберігаються у t.
2. Засліплення відкритих даних c.
3. Рандомізація секретних даних b.

Мета цієї статі полягає не тільки в аналізі запропонованих методів протидії атакам спеціального виду, а ще й у знаходженні таких методів, реалізація яких не впливала б на ефективність самого алгоритму, тобто щоб алгоритм не втрачав своєї початкової швидкості, стійкості, ефективності.

Загальним принципом впровадження методів є рандомізація та складність вияву залежності операції над значенням секретних даних, важливим аспектом реалізації кожного методу протидії є необхідність підтримувати початкові властивості алгоритму: швидкість, стійкість, ефективність.

Використовуючи класифікацію атак спеціального виду на енергоспоживання[3], проаналізуємо запропоновані методи протидії для криптосистеми NTRU.

4.РАНДОМІЗАЦІЯ ТИМЧАСОВИХ ДАНИХ, ЯКІ ЗБЕРІГАЮТЬСЯ У *t*

Першим методом протидії є ініціалізація t з випадковими цілими числами, а не нулями. Ця протидія направлена як на SPA, так і на CPA(включаючи DPA). Ініціалізація t з невідомими значеннями ускладнює для зловмисника реалізацію SPA та робить складнішим пошук кореляції між енергоспоживанням та основним додаванням, тому що один з двох операндів має випадкове значення. Тобто імовірність знаходження максимумів, в ході аналізу спектра енергоспоживання зловмисником, йде до нуля, що і потрібно було зробити.

На рис. 1 показано максимальне значення коефіцієнта кореляції після використання першого заходу протидії, з цього можна зробити висновок, що пошук максимального піку для визначення значення $b[l]$-$b[l$-1] є досить складним.

Для того щоб реалізація алгоритму не втратила необхідну ефективність, необхідно щоб $t_{\max} \le d \times \max_{0 \le k < N} c_k$, де t_{max} – є максимумом серед t при $0 \le j \le 2N$.

Таким чином впровадження цього заходу тільки обмежить стійкість алгоритму до CPA, оскільки обмежується вибір r_j. Наприклад, шукаючи вихідне значення $b[1]$-$b[0]=3$ (див. рис.1), зловмисник має $HD(c_3, c_3+c_0)$ та це значення зміниться на $HD(r_4+c_3, r_4+c_3+c_0)$, у випадку реалізації першої протидії. Тоді буде безглуздо використовувати r_4, який набагато більший, ніж c_3+c_0, тому що з високою імовірністю положення старшого біту в r_4 майже не сприяє знаходженню відстані Хеммінга, для цього c_3+c_0. Тому розумно припустити, що r_4 знаходитиметься в інтервалі $[0, c_3+c_0]$. Просте узагальнення цього спостереження для інших значень $b[l]$-$b[l$-1] призводить до рішення, що розумно припустити, що $r_j \le t_{\max}$. Якщо $\max_{0 \le k < N} c_k$ у звичайному шифр-тексті, то $r_j < dq$.

Після цього зловмисник може зробити припущення щодо деякого фіксованого значення

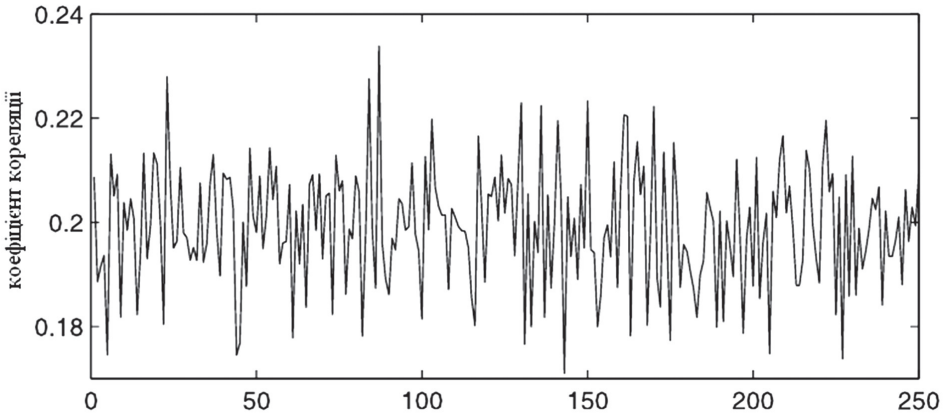

Рис. 1. Максимальна кореляція для кожного можливого припущення після впровадження протидії №1

всіх r_j при $r < dq$ та спробувати розпочати схожу атаку до оригінального CPA. Такий вид атаки може бути визначений як потенційний, тому що у випадку, коли зловмисник накопичив достатнє число слідів енергоспоживання, він матиме багато випадків, де $r_{b[l]} = r$ і випадок, коли всі інші стани відіграватимуть роль шуму. Однак, виникає проблема, що кожне r_J впливатиме тільки на одне t_j протягом виконання алгоритму. Таким чином, якщо наведена вище атака успішна для розкриття $b[1]$-$b[0]$, то вона також може бути використана для знаходження усіх значень $b[l]$-$b[l\text{-}1]$, без істотного збільшення числа потрібних слідів енергоспоживання.

5. ЗАСЛІПЛЕННЯ ВІДКРИТИХ ДАНИХ *c*

Розглядаючи цей метод, можна запропонувати два варіанта цього методу: рандомізація цілих чисел та рандомізація поліному. Перший реалізує рандомізацію цілого *r* та неодноразово використовується для засліплення всіх $c_к$. Цей захід протидії маскує кореляцію між поліномом $c(X)$ та енергоспоживанням рандомізованого $c(X)$. Насправді, ця процедура має такий вигляд $(c(X)+R(x))*a(X)-R(X)*a(X)$, де $R(X)=[r,r,..,r]$. Оскільки $R(X)*a(X)=[dr \mod q, dr \mod q,...,dr \mod q]$, то можемо ліквідувати $R(X)*a(X)$ шляхом віднімання dr від кожного t_j.

Цей метод можна назвати досить прийнятним за рахунок незначних накладних витрат. Однак, потрібно бути обережними при використані засліплення у ситуації, коли енергоспоживання обчислюється за допомогою коду Хеммінга, тому що інший вид атаки CPA теоретично буде можливим у цьому випадку. Наприклад, вважатимемо, що енергоспоживання змінюється від найменш значущого біта кожного t_j. Спочатку пояснимо атаку CPA проти алгоритму без використання протидій. Як зазначалося вище, завдання зловмисника полягає у знаходженні вихідного відносного зсуву індексу *t*, яке показує $b[1]$- $b[0]$, $b[2]$-$b[1]$ і т. д. Тому візьмемо поліном $c^1,...,c^S$ та його сліди енергоспоживання $P^1,...,P^S$ зробимо припущення, що $b[1]$-$b[0]=w$ при $w \geq 1$, та перевіримо на наявність помітних кореляцій між $LSB(c_w^l + c_0^l)$ та P^l, де $LSB(x)$ – значення найменш значущого біта *x*. Цікавий факт те, що ця атака буде реалізована навіть якщо *r* додане до кожного $c_к$, $LSB((c_w^l + r)+(c_0^l + r)) = LSB(c_w^l + c_0^l)$. На рис. 2 показано, що пік з'являється серед коефіцієнтів кореляції, хоча це важко зробити на рис. 3, тому що енергоспоживання нашого процесору впливає більш швидше на відстань Хеммінга, ніж на код Хеммінга.

Решта завдання атаки, відновлення $b[2]$-$b[1]$, $b[3]$-$b[2]$ і т. д., ускладнюється в результаті втрати залежності *r* на *LSB*. Ця проблема може буде легко вирішена припущенням двох відносних зсувів водночас. Вважатимемо, що зловмисник

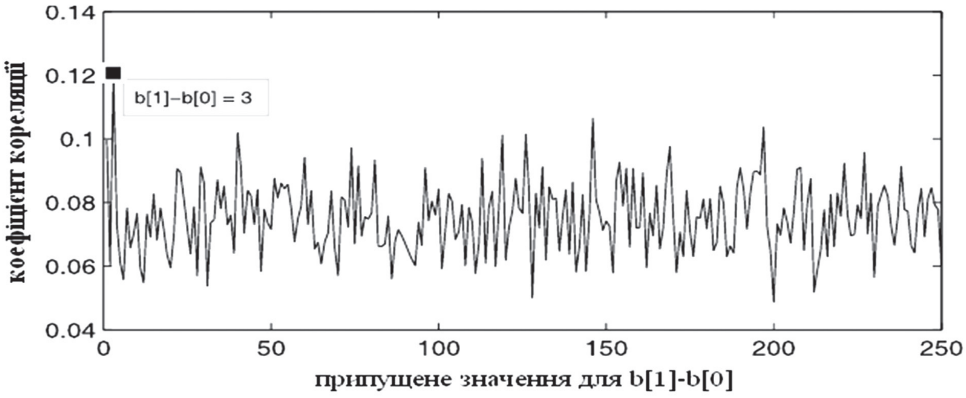

Рис. 2. Максимальна кореляція для кожного можливого припущення при моделі коду Хеммінга з *c*, який засліплений випадковим цілим числом

відновив $b[1]$-$b[0]=v$, використовуючи вищезазначений метод. Після чого зловмисник робить припущення $b[3]$-$b[1]=w_1$ та $b[3]$-$b[1]=w_2$ та знаходить кореляцію, використовуючи $LSB(c_{w_1+v}+c_{w1}+c_{w2}+c_0)$. Наприклад, v=3, w_1=3, w_2=2, див. рис. 2 [3]. Цей метод успішно ліквідовує ефект засліплення для r, тому що значення, з яким зловмисник має справу, складається з парного числа r. Хоча простір пошуку (w_1, w_2) буде більшим, ніж просте w, він все ще знаходиться у практичному діапазоні. Тому, розглядаючи перший метод з простим цілим r, можна вважати потенційним рішенням для розв'язання задачі рандомізації відкритих даних.

Розв'язати цю задачу може і наступний метод, він оснований на використані загального поліному $R(X)$, який безпосередньо і буде засліплюватиме $c(X)$. Вирахуємо $(c(X)+R(X))*a(X)$-$R(X)*a(X)=c(X)*a(X)$, використовуючи випадковий поліном $R(X)$. Для зменшення навантаження обчислення $R(X)*a(X)$ взяли за ідею [5] та [6]. Тобто спочатку обирається випадкове $R(X)$, обчислюється $S(X)=R(X)*a(X)$, та зберігається $R(X)$ та $S(X)$. Коли згортання $(c(X)+R(X))*a(X)$- $S(X)$ буде зроблено, $R(X)$ та $S(X)$ оновлюється шляхом обчислення $R(X) \leftarrow kR(x)$ та $S(X) \leftarrow kS(x)$ для випадкового κ. Тому можна використовувати другий метод як ефективну протидію проти CPA. На рисунку 3 показано максимальне значення коефіцієнта кореляції після застосування цієї протидії. Але все одно знаємо, що засліплення c не перешкодить реалізації SPA атаки.

6. ВИСНОВКИ ВІДНОСНО АТАКИ ДРУГОГО РОДУ

Проаналізувавши запропонований захід протидії, а саме рандомізацію вектора r_k, зловмисник може зробити висновок про ймовірність реалізації атаки CPA. Тобто є ймовірність того, що рандомізацію вектора r_k можна відокремити від сигналу енергоспоживання для отримання корисної інформації.

Спочатку розглянемо сутність атаки CPA. Завдання зловмисника полягає у відновленні $b[1]$-$b[0]$ для отримання множини b. Для цього зловмисник описує вираз енергоспоживання, використовуючи модель відстані Хеммінга(1), робить припущення P відносно значення енергоспоживання, тобто значення регістра, що змінюється під час виконання операції згортання поліномів.

$$P(y \to z) \approx mHD(y,z)+n = mHW(y \oplus z)+n, \quad (1)$$

де m – скалярний коефіцієнт посилення між відстанню Хеммінга та енергоспоживанням і n – незалежна зміна шуму.

Повернемося до рисунка 1 [3], де розглянуто приклад, за яким зловмисник робить припущення w відносно значення $b[1]$–$b[0]$. Його припущення будується на відстежуванні відмінностей кореляції між $P(r_k \to r_k + c_w)$ та $HD(r_k, r_k + c_w)$ при j=0 та кореляції між $P(r_k + c_w \to r_k + c_w + c_0)$ та $HD(r_k + c_w, r_k + c_w + c_0)$ при j=1. Усі припущення зловмисника можна подати у вигляді

$$HW(x \oplus (x+y)) \quad (2)$$

та звести до

$$HW(x \oplus (x+y)) = HW(y)+\epsilon, \quad (3)$$

де ϵ – імовірнісна залежність зсувів при операції згортання поліномів з використанням рандомізації вектора r_k.

Таким чином, у випадку, коли зловмисник отримав достатньо статистичних даних про операції згортання на деякій множині поліномів, він, проаналізувавши енергоспоживання отриманих операцій згортання та використовуючи вирази (1) та (2), може припустити, що можна знайти залежність зсувів при використанні рандомізованого вектора r_k. Це припущення сформоване на підставі складності вибору r_k та переповненні або переносі регістра зсуву при додаванні r_k до добутку поліномів. Потім зловмисник відфільтровує шум, маючи на увазі корисну інформацію про рандомізований вектор r_k, та отримує сигнал даних енергоспоживання операції згортання без реалізації заходів протидії атакам на енергоспоживання, проводить атаку спеціального виду [3], тим самим відновлюючи секретний ключ.

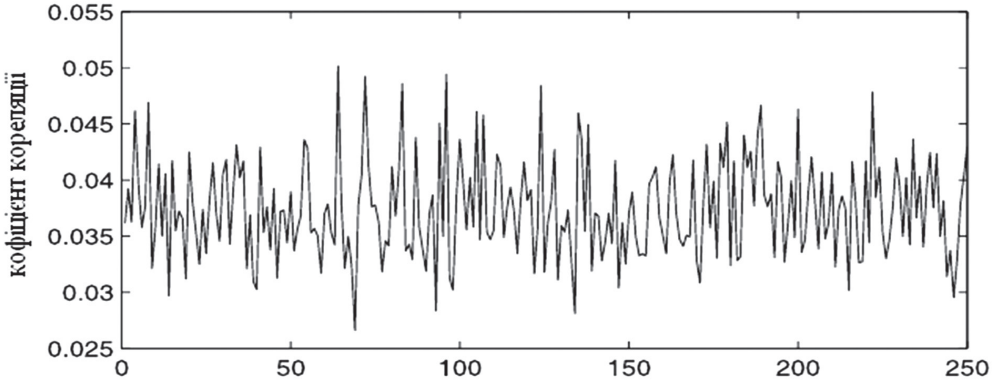

Рис. 3. Максимальна кореляція для кожного можливого припущення з c, який засліплений випадковим поліномом

7. РАНДОМІЗАЦІЯ *b*

Під час спостережень за поведінкою алгоритму 1 виявився цікавий факт, що зміна порядку елементів множини *b* не впливає на результат операції згортання. Цей факт відкриває ефективність використання рандомізації *b*, як міри протидії атаці CPA. Ця протидія може ефективно запобігти CPA, тому що CPA використовує позиції відносних зсувів, які додаються до c_0 між двома послідовними операціями в головному циклі, але мета порівняння та значення цих зсувів змінюється цією протидією при кожному виконанні. Наприклад, при ітерації $j = 0$ та $j = 1$, відносний зсув більше не дорівнює $b[1] - b[0]$, крім того він більше немає фіксованого значення. На рисунку 4 показано максимальне значення коефіцієнтів кореляції після застосування рандомізації *b*.

Проте необхідно відмітити, що рандомізація *b* може мати потенційну слабкість до SPA атаки, якщо зловмисник зробить декілька успішних припущень.

Нехай множина $b'[j]$ є елементом в *j* позиції *b* після перестановки. Тоді легко помітити, що пара ($b'[1]$, $b'[0]$) може мати $d(d–1)$ варіантів, тобто 2^{256} варіантів при $d = 48$. Якщо зловмисник зібрав достатнє число слідів енергоспоживання, то всі $d(d–1)$ варіанти також мають бути включені до зібраних даних.

Потім зловмисник представляє атаку SPA незалежно для кожного з слідів енергоспоживання, відновлюючи упорядковану множину *B* усіх можливих значень при відносному зсуві $b'[1] – b'[0]$. Хоча ця множина *b* не явно показує оригінальну множину *b*, але може показати деяку частину інформації про *b*, якщо *b* буде вибрано не обережно. Наприклад, вважатимемо, що при N=251 та d=48 останні елементи множини *B* матимуть вигляд [239,242,244,245,246,249]. Потім останній елемент 249 інформує зловмисника, що ($b[0]$,$b[47]$)=(0,249) або (1,250), тому що максимальний зсув має відбутися між $b[1]$ та $b[d\text{-}1]$. Це означає, що зловмисник відновить два вихідних елемента з 48-ми з імовірністю 0,5, та ця процедура може бути продовжена для визначення інших елементів, сконструювавши дерево пошуку(див. рис. 5). Для простоти пояснимо тільки першу гілку, тому що інша буде симетричною. Другий останній елемент у *B,* 246, породжує 3 дочірні гілки у дереві пошуку. Тобто ($b[0]$,$b[1]$,$b[46]$, $b[47]$)=(0,3,246,249); ($b[0]$,$b[1]$,$b[47]$)=(0,3,249) та $b[46] \neq 246$ ($b[0]$,$b[1]$,$b[46]$)=(0,3,246) та $b[1] \neq 3$. Але перша гілка може бути скорочена, тому що перша гілка не входить до множини *B* у точці, в якій зловмисник не може знайти відносний зсув $b[46]$-$b[1]$=243 у *B.* Виходячи з цього на наступному рівні, зловмисник отримує 4 секретних елемента з 12 варіантів, що істотно знижує пошук у просторі *b*. Хоча такий вид атаки буде корисний тільки при невеликій глибині дерева, тому що утворюється велика кількість гілок після певного рівня і обрізка практично неможлива, тому потрібно бути обережним при використанні такої протидії проти атак SPA.

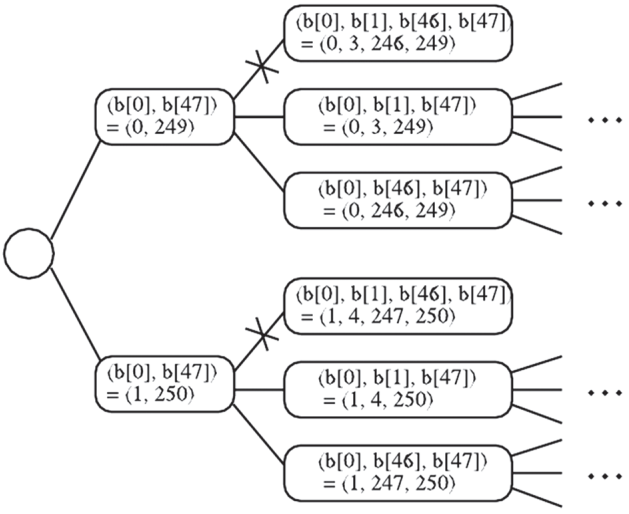

Рис. 5. Приклад дерева пошуку при B = [...,239,242,244,245,246,249]

8. АНАЛІЗ ПРОДУКТИВНОСТІ

Аналізуючи методи протидії, доцільно було б порівняти алгоритм [1] та алгоритми з різними методами протидії. На нашу думку ці реалізації можна порівняти, аналізуючи використану пам'ять та швидкість операції обчислення, тобто, доказуючи ефективність протидії до розглянутих атак, потрібно також враховувати вплив реалізації методів на властивості алгоритму.

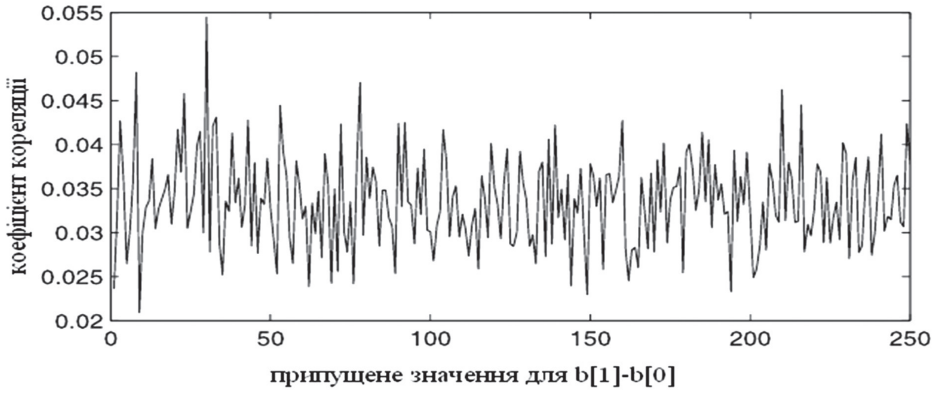

Рис. 4. Максимальна кореляція для кожного можливого припущення з рандомізованим *b*

Розглянувши табл. 1, можна проаналізувати продуктивність різних реалізації щодо виконання операції згортання $t(X)=c(X)*a(X)$, яка є вразливою до атак спеціального виду на енергоспоживання. Як видно з таблиці, що засліплення *c* з випадковим поліномом вимагає занадто багато пам'яті в порівнянні з іншими заходами протидії та більше використовує обчислювальний ресурс ніж інші заходи. Засліплення *c* з випадковим числом показує найвищу швидкість серед усіх заходів, але цей метод вразливий до атак типу CPA. Далі з таблиці видно, що порівнюючи використання пам'яті та швидкості обчислення, можна виділити реалізацію одночасно двох заходів: рандомізація *t* та рандомізація *b,* реалізація яких зведе нанівець можливість CPA та SPA.

Таблиця 1

Алгоритм згортання	ROM	RAM	Затрачений час
Алгоритм 1 (без застосування протидії)	3796	1063	67.383
Рандомізація *t*	3980	1063	71.191
Засліплення *c* з цілим *r*	4022	1064	69.043
Засліплення *c* з поліномом *R(X)*	4194	2067	101.953
Рандомізація *b*	4050	1063	70.117
Рандомізація *t* та рандомізація *b*	4106	1064	73.828

ВИСНОВОК

Таким чином, проаналізувавши методи протидії, виявили, що кожний метод має як переваги, так і недоліки, і назвати універсальний метод протидії, який би протидіяв однаково ефективно атакам спеціального виду, виявилося складно. Насамперед, методи ускладнюють завдання зловмисника з відновлення секретного ключа, але при реалізації методів протидії потрібно значну увагу приділяти впливу цих методів на сам алгоритм.

Рандомізація *t* ускладнює SPA та робить складнішим пошук кореляції, але обмежується вибором r_j, що може призвести до потенційних атак. Засліплення *c* може реалізовуватися двома варіантами, нести незначні накладні витрати, але вразливі до атак, які використовують для аналізу даних код Хеммінга, та при реалізації засліплення *c* за допомогою поліному потрібно більше RAM(вдвічі більше, ніж у інших випадках). Рандомізація *b* ефективна проти CPA, але не ефективна проти SPA, при атаці SPA – контролюючі вхідні дані та використовуючи дерево пошуку, буде досить легко знайти залежності та досягнути мети.

Література

[1] Hoffstein, J. "NTRU: A new high speed public key cryptosystem,"/J. Hoffstein, J. Pipher, J. Silverman Preprint// presented at the rump session of Crypto 96.

[2] Іваненко Д.В. Порівняльний аналіз сучасних асиметричних криптосистем/Д.В. Іваненко, О.В. Сєвєрінов//Системи управління, навігації та зв'язку. – К: ЦНДІ НіУ, 2012. – Вип.2(22).

[3] Іваненко Д.В. Класифікація атак спеціального виду на енергоспоживання/Д.В. Іваненко//Системи обробки інформації. – Х.: ХУПС, 2012. – Вип. 5 (103).

[4] Hoffstein J. "Optimizations for NTRU,"/ J. Hofftein, J. Silverman,// Proc.Public-Key Cryptography and Computational Number Theory,2000.

[5] Coron, J.S. "Resistance against differential power analysis for elliptic curve cryptosystems," / J.S.Coron, // Cryptographic Hardware and Embedded Systems — CHES'99, LNCS, vol.1717, pp.292–302, Springer, 1999.

[6] Okeya K., "Power analysis breaks elliptic curve cryptosystems even secure against the timing attack,"/ K.Okeya, K. Sakurai // Indocrypt 2000, LNCS, vol.1977, pp.178–190, Springer, 2000.

[7] Brier E. "WeierstraЯ elliptic curves and side-channel attacks,"/ E. Brier, M. Joye // Public Key Cryptography — PKC 2002, LNCS, vol.2274, pp.335–345, Springer, 2002.

[8] Fischer W., "Parallel scalar multiplication on general elliptic curves over Fp hedged against non-differential side-channel attacks,"/ W. Fischer, C. Giraud, E. Knudsen, J. Seifert // 2002. International Association for Cryptologic Research (IACR) Cryptology ePrint Archive 2002/007, http://eprint.iacr.org/2002/007.

[9] Izu T., "A fast parallel elliptic curve multiplication resistant against side channel attacks,"/ T. Izu, T.Takagi // Public Key Cryptography — PKC 2002, LNCS, vol.2274, pp.280–296, Springer, 2002.

[10] Okeya, K., "Elliptic curves with the montgomery-form and their cryptographic applications,"/ K. Okeya, H. Kurumatani, K. Sakurai,// Public Key Cryptography — PKC 2000, LNCS, vol.1751, pp.238–257, Springer, 2000.

[11] Liardet P. "Preventing SPA/DPA in ECC systems using the Jacobi form,"/ P. Liardet, N. Smart // Cryptographic Hardware and Embedded Systems — CHES 2001, LNCS, vol.2162, pp.391–401, Springer, 2001.

[12] Joye M. "Hessian elliptic curves and side-channel attacks,"/ M. Joye. J. Quisquater // Cryptographic Hardware and Embedded Systems — CHES 2001, LNCS, vol.2162, pp.402–410, Springer, 2001.

[13] Bernstein D., "Faster addition and doubling on elliptic curves," / D.Bernstein, T. Lange //Advances in Cryptology — Asiacrypt 2007, LNCS, vol.4833, pp.402–410, Springer, 2007.

[14] Chevallier-Mames B. "Low-cost solutions for preventing simple side-channel analysis: Side-channel atomicity,"/ B. Chevallier-Mames, M. Ciet, M. Joye,// IEEE Trans. Comput., vol.53, no.6, pp.760–768, 2004.

[15] Oswald E., "Randomized addition-subtraction chains as a countermeasure against power attacks,"/ E. Oswald, M. Aigner, // Cryptographic Hardware and Embedded Systems — CHES 2001, LNCS, vol.2162, pp.39–50, Springer, 2001.

[16] Moeller B., "Securing elliptic curve point multiplication against side-channel attacks,"/ B. Moeller // Information Security — ISC 2001, LNCS, vol.2200, pp.324–334, Springer, 2001.

[17] Hasan M., "Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems,"/ M. Hasan // IEEE Trans. Comput., vol.50, no.10, pp.1071–1083, 2001.

[18] Lee, M.K., "Sliding window mothod for NTRU,"/ M.K. Lee, J.W. Kim, J.E. Song, K. Park // Applied Cryptography and Network Security — ACNS 2007, LNCS, vol.4521, pp.432–442, Springer, 2007.

[19] Gama N., "Symplectic lattice reduction and NTRU,"/ N. Gama, N. Howgrave-Graham, P. Nguyen // Eurocrypt 2006, LNCS, vol.4004, pp.233–253, Springer, 2006.

Надійшла до редколегії 26.04.2013

Іваненко Дмитро Вікторович, аспірант кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки. Наукові інтереси: криптографія, криптоаналіз.

УДК 621. 391:519.2:519.7

Методы противодействия атакам специального вида на криптопреобразования NTRU, которые основываются на анализе энергопотребления / Д.В. Иваненко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 292–298.

Анализируются существующие методы противодействия атакам специального вида, которые основываются на анализе энергопотребления. Рассматривается реализация атак специального вида на криптопреобразования NTRU, учитывая реализованные методы противодействия, такие как рандомизация и заслепление. Проведен анализ недостатков и преимуществ методов противодействия относительно таких атак специального вида как SPA, DPA и CPA, которые были направлены на криптопреобразования NTRU.

Ключевые слова: методы противодействия, атаки специального вида, CPA, DPA, SPA.

Табл.: 1. Ил.: 5. Библиогр.: 19 назв.

UDC 621. 391:519.2:519.7

Methods to counteract side channel attacks on the NTRU cryptotransformations, based on energy consumption analysis / D.V. Ivanenko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 292–298.

The paper analyzes methods of counteracting side channel attacks which are based on energy consumption analysis. Implementing side channel attacks on NTRU cryptotransformation is considered taking into account the realized methods of counteracting such as randomization and blinding. Analyzing advantages and disadvantages of the methods of countracting such side channel attacks as CPA, SPA and DPA which were aimed at NTRU transformations is performed.

Keywords: methods of counteract, side channel attacks, CPA, SPA, DPA.

Tab.: 1. Fig.: 5. Ref.: 19 items.